VeriSign®

WHITE PAPER

Security in the Any Era:
Balancing Risk, Cost, and the User Experience

CONTENTS

Security in the Any Era:
Balancing Risk, Cost, and the User Experience

+ Executive Summary

The Internet has matured from a phenomenon to a transformational infrastructure that is changing our society. Consumers can conduct business from virtually anywhere, and they increasingly expect companies to provide access to services, content, and information anytime, from any device. As enterprises open and extend their networks to accommodate the demands of this "Any Era," threats and vulnerabilities increase. These threats target the key assets of online business: consumers, brands, Web sites, and internal networks. When attacks on these assets occur, they undermine consumer confidence and growth of the digital economy. VeriSign offers a layered, systematic approach to mitigating threats to Any Era assets. Using this approach, complementary security layers fortify each other to create a solution that is stronger than the sum of its parts, while making the user experience as rich and seamless as possible.

+ The Any Era: Consumer-Driven, Always Available Service

Recent technology improvements, the expansion of Internet Protocol (IP) networks, and mass adoption of the Internet and wireless devices have induced a cultural transformation. Our society is increasingly shifting from physical interaction to digital interaction, and this shift is changing how people work, live, and play. Online social-networking communities, shopping, banking, bill payment, and entertainment are part of daily life. At the same time, online services and information are giving consumers (whether individuals, organizations, partners, or suppliers) more choice and more control over who gets their business. Companies can no longer dictate how, where, and when to deliver their services and products; they can't even restrict offerings to one-size-fits-all. In addition, companies must be prepared to handle unexpected spikes in usage, as consumers migrate in large numbers to digital services. Consumers are in charge, and they expect easier, more integrated access to personalized information, entertainment, content, and commerce anytime, from anywhere, via any channel, network, or device. To remain competitive in this new "Any Era," today's businesses must provide an exceptional online experience that meets these demands quickly, conveniently, and *securely*—with minimal complexity or cost to the consumer. Security and consumer trust are vital to maximizing opportunity.

Maximizing Opportunity by Building Consumer Trust

Although online usage has climbed steadily in recent years, consumers still have legitimate concerns about identity theft, credit card data breaches, phishing scams, counterfeit products sold online, and other security issues. These concerns overshadow the user experience and dampen consumption of online services and products. In one study, 53% of online consumers stated that concerns about breaches had affected their purchasing behavior. The same study shows that online sales are a net positive for retailing (i.e., they don't just cannibalize but increase overall sales), yet more than $2 billion in sales probably did not occur last year because of security concerns.[1]

[1] 2007 Gartner, Inc. Trends in Consumer Security

To take full advantage of the productivity and revenue opportunities presented by the Any Era, businesses must increase consumer trust and usage. They must protect not only consumers, but also their brands, networks, and Web sites, and they must ensure that all online content, communication, and commerce remains secure at every layer of transmission and storage. Consumers have access to multiple sources of information, and any security breach—even if it does not affect consumers directly—raises doubts about a company's overall security posture.

Key Business Assets of Any Era Networks

Online businesses must protect the following categories of assets in order to create a more secure end-to-end user experience: consumers, brands, Web sites, and networks. End-to-end security is necessary not only to preserve consumer trust and encourage online usage, but also to avoid financial losses and regulatory penalties.

+ Consumers

Consumers are one of a company's most valuable assets, and maintaining their trust is paramount. Regardless of how, when, or why consumers access the Internet, companies must be able to secure their transactions and verify their identity as transparently as possible. Doing so helps protect consumers' online information from identity theft, fraud, and unauthorized access to confidential data. Because passwords are highly vulnerable to compromise, passwords and user IDs alone are rarely sufficient for high-value interactions. Multi-factor authentication combined with server-side fraud monitoring and protection provides a stronger solution, and can be used with a variety of credentials such as smart cards, tokens, and cell phones.

According to results of an extensive survey conducted by the U.S. Department of Justice, identity thieves victimized 3.6 million households, representing three percent of the population, in one six-month period. In addition, identity theft costs about $US 6.4 billion per year. (U.S. Department of Justice, National Crime Victimization Survey 2004, www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm, published April 2006)

+ Brands

Brand trust and loyalty are critical to a company's success—especially for financial institutions, pharmaceutical companies and healthcare organizations, and e-commerce sites. Negative sentiment, consumer activism, counterfeit goods, theft of intellectual property, typo squatting (redirection of traffic using a known brand to attract consumers), phishing, and other forms of brand abuse can destroy hard-earned credibility, divert customers to illegitimate sites where fraud may be committed, and drain revenue. To protect brands, companies must have early warning systems to detect and thwart fraud attempts. They must also be able to manage, monitor, and respond quickly to reputation, phishing, and counterfeiting threats.

As many as one in ten IT products sold globally may actually be counterfeit, which equates to $US 100 billion in lost IT revenue. (KPMG, Managing the Risks of Counterfeiting in the Internet Technology Industry, www.kpmg.co.uk/pubs/050274.pdf as of 3/21/07).

In developing countries, up to 50% of imported drugs are estimated to be counterfeit, endangering the health of consumers and diverting revenue from pharmaceutical companies. (Ibid KPMG)

Phishers use email spam and Internet resources to wage phishing attacks, in which they impersonate legitimate businesses and Web sites in order to obtain personal, high-value information from unsuspecting consumers. The intent is to use the information for financial gain (e.g., fraud or identity theft).

+ Web Sites

Companies must protect their Web sites in order to ensure that their brands, customers, and transactions are not compromised by phishers, hackers, unauthorized users, or other malicious actors. Besides ensuring that only authorized users can access site resources, companies must provide prominent visual cues to help users quickly determine that a Web site is legitimate. Most Internet users are familiar with the tiny lock icon that appears on pages that have been encrypted by Secure Sockets Layer (SSL) Certificates. They may also know that the "https" in their browser's address bar indicates that the site has authenticated itself with an SSL certificate. However, these elements alone do not indicate who issued the SSL Certificate or whether the certificate is trustworthy. Extended validation (EV) SSL Certificates provide additional cues that help to extend trust online, such as turning the address bar green or displaying the name of the certificate owner.

> The number of phishing attacks grew from 15,050 in June 2005 to 29,930 in January 2007, a nearly 100% increase in 19 months (Anti-Phishing Working Group, Phishing Activity Trends, March 2007).

+ Internal Networks and Application Infrastructure

The network is a company's core business IT asset. As companies open their networks to not only customers, but also business partners and development shops throughout the world, the number of access points increases—and so do the opportunities for exploitation. Adding to the challenge is the increase in compliance requirements dictated by the Sarbanes-Oxley Act, the payment card industry, the FFIEC, and other regulatory bodies.

Threats to the network and applications can originate from many sources outside or inside the firewall. Employees can accidentally or intentionally introduce denial of service (DOS) attacks, adware, spyware (malicious code that tracks victims' online activity), viruses, and other malicious code. Passwords can be compromised. Security policies may be enforced inconsistently. Improperly integrated security systems and other hardware and software configurations may also expose the system.

Compounding the problem, hackers and the attacks they wage have changed significantly over the past few years. Hackers are developing malicious code more quickly, and they are becoming more technically sophisticated in the way they circumvent network controls such as anti-virus software and firewalls. Their attacks are stealthier and more targeted, affecting specific industries, organizations, groups, individuals, and product sets. And, whereas the chance for notoriety once motivated them, today's hackers often seek financial gain or revenge.

VeriSign identified 16,627 unique malicious codes in 2005, a 62% increase over the preceding year.

Piecemeal Asset Protection

As companies modify their infrastructure to provide legitimate users with easier, more integrated access to data of all kinds, they must protect every layer of assets—consumers, brands, Web sites, and networks. Although security technology exists to protect specific assets of Any Era businesses, no single product or product suite provides a total security solution—and no combination is foolproof. Companies are often faced with cobbling together dozens of point products and services to create a piecemeal solution that offers only partial security to parts of the overall infrastructure. These reactive, one-dimensional solutions often increase complexity, cost, and risk. In-house personnel must integrate, test, and maintain disparate systems, and they must make significant investments in training. Economies of scale are lost by working with multiple vendors and maintaining multiple service level agreements. And system incompatibilities, policy oversights, and integration errors introduce security holes and vulnerabilities. In addition, intelligence gathering capabilities are rarely as robust as those provided by outside security consultants and managed service providers, who tend to have faster, more global access to information about network vulnerabilities, impending attacks, and solutions.Even when all products or product suites are operating correctly, point solutions cannot adequately address the Any Era user-experience paradigm or protect the multiple layers of online business assets that comprise the Any Era ecosystem. They simply lack the foundation, coordination, and resources to deliver the skill set, technology, global intelligence, or third-party trust that the Any Era requires.

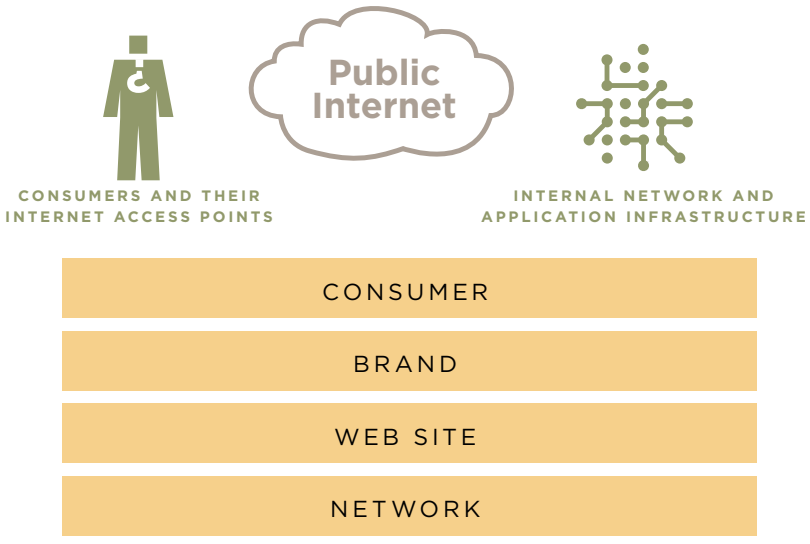
+ The VeriSign Approach: Layered Security

VeriSign operates digital infrastructure that enables and protects billions of interactions every day across the world's voice and data networks. VeriSign runs the infrastructure that supports the world's *.com* and *.net* domains, protects over 93% of the Fortune 500's Web properties, manages over 5,000 security devices on behalf of worldwide enterprises, and monitors over 2 billion security events every day.

VeriSign approaches asset protection differently. Instead of point solutions, VeriSign uses a systematic, layered approach to security that includes end-to-end services and expert assistance in enabling and protecting networked interactions. "Layered security" acknowledges that a foolproof solution is probably not achievable, but that proper tradeoffs between risk, cost, and user experience in selecting security products and services can result in the best security solutions to protect a company's consumers, brand, Web properties, and network. When developing and implementing a layered defense, VeriSign consultants work with the company's existing infrastructure and third-party technology and service providers to provide the best solution for a company's unique assets. VeriSign considers not only the company's security needs, but also its overall business and the end-to-end user experience. By layering multiple integrated technologies, VeriSign's layered defense provides a cumulative effect that offers as secure a solution as practical when risk, user experience, and cost are weighed. In addition, the VeriSign services model saves companies time and money by allowing them to focus their resources on core business objectives.

VeriSign's layered defense solutions help protect all the online business assets required for networked interactions, including consumers, brands, Web sites, and internal networks.

Figure 1: VeriSign's Layered Defense Solutions



Consumer Identity Protection and Fraud Prevention

VeriSign's layered authentication solution combines strong user authentication and intelligent fraud monitoring and detection to provide in-depth defense—while minimizing impact on the user experience. Two services help ensure that a user is who he or she claims to be: VeriSign® Identity Protection (VIP) Fraud Detection Service and VIP® Authentication Service. Based on open standards, both services are OATH-compliant to help support strong authentication across all users, all devices, and all networks. Unlike shared-secret based authentication (in which the site authentication and the user authentication are linked) the services operate independently of each other, providing more autonomous verification.

VIP Fraud Detection Service provides invisible server-side fraud monitoring and fraud detection. By leveraging Internet fraud experience, state-of-the-art technology, hands-on analysts, and an intelligent network to identify fraud patterns and anomalies, the service bases decisions on more comprehensive data than a simple shared-secret mechanism.

VIP Authentication Service provides standards-based two-factor authentication and includes options for supplemental factors, including standalone hardware devices such as one-time password (OTP) tokens and "soft" devices such as voice-enabled tokens, mobile device tokens, and SMS OTP. Authentication mechanisms are linked to a network that binds one identity to multiple parties in the network, so that users can use a single device to access multiple services.

Brand Monitoring

VeriSign's multi-layered approach to brand protection includes domain management as well as monitoring, detection, and response services that help companies quickly identify and resolve issues that affect their digital brand and reputation. VeriSign® Brand Protection Services include monitoring and detection mechanisms that provide early warning of potential counterfeiting, phishing, brand abuse, or affiliate non-compliance activity and enable analysts to respond rapidly and effectively to incidents —even when take-down action is necessary. The services use two related strategies to ensure that companies receive well-distilled, relevant, and organized results. First, the services custom-build all incident detection and prioritization capabilities according to the unique business needs of the company and industry. Second, the services prioritize legitimate incidents by evaluating the *context* in which they occur. Built on VeriSign's proven infrastructure and strengthened by VeriSign's global relationships and seasoned analysts, these services help organizations protect revenue, lower operational costs, and preserve consumer, supplier, and partner confidence—all while alleviating the burden associated with an in-house brand monitoring infrastructure.

Extended Validation (EV) SSL Certificates for Web Site Verification

To enable consumers to easily identify legitimate sites, VeriSign layered defense solutions offer extended validation (EV) SSL certificates. When a site uses an EV certificate to authenticate itself, the consumer's browser displays easily understood visual cues to provide tangible assurance of a site's authenticity. The address bar turns green, a large lock icon appears next to the address, and the certificate issuer's name is displayed. This functionality is based on open standards and is present in all current Microsoft browser versions, including Internet Explorer 7. More than 400 large organizations in North America are deploying EV SSL certificates, and VeriSign anticipates that most major e-commerce sites and Microsoft will educate their end users about EV certificates, making this mechanism a universally recognized tool for authentication. The VeriSign Seal provides an additional visual cue to users. Any customer using VeriSign-issued SSL certificates can place the Seal on its SSL-secured pages. Research indicates that users react very positively to the Seal as VeriSign is the most widely recognized security brand by Internet consumers.

Multi-Pronged Network Defense

VeriSign leverages an extensive intelligence-gathering network, proven methodology, state-of-the-art tools, and highly skilled professionals to deliver comprehensive, multi-layered defense against network-based security threats and vulnerabilities. Using these resources, companies can gauge risk more accurately and respond rapidly and appropriately to protect business-critical data and systems. VeriSign's layered network defense includes a variety of services, including (but not limited to):

+ **Security assessments and compliance consulting** (VeriSign® Global Security Consulting)
+ **Context-based threat intelligence** (VeriSign® iDefense Security Intelligence Service)
+ **Managed firewall and intrusion prevention services with advanced event correlation** (VeriSign® Managed Security Services)
+ **Managed Domain Name System services** (VeriSign® DNS Assurance)
+ **Enterprise authentication for employees and business partners** (VeriSign® Unified Authentication)
+ **Secure mobile device management** (VeriSign® Mobile Device Management Services)

This multi-faceted approach gives companies a holistic network security solution that allows them to optimize existing resources while comprehensively managing risk.

Real-World Expertise

VeriSign® Global Security Consulting leverages exceptional regulatory knowledge, vendor neutrality, subject matter expertise, business acumen, and unique intelligence gathering capabilities to tailor practical, layered defense solutions that help protect a company's assets, while making the best use of existing in-house personnel, technology, and processes. VeriSign security professionals are trained, certified, and experienced in the design, acquisition, and deployment of all major security solutions. With an average of ten years' experience in enterprise information security, and many with multiple security and audit certifications, VeriSign consultants demonstrate expertise across the entire information security and privacy spectrum.

The VeriSign consulting team complements skill and training with proven, real-world experience. Forty percent of VeriSign Global Security Consulting engagements center on security assessments, and most consulting service customers are in regulated industries (mainly financial services, healthcare, and retail). VeriSign security professionals encounter a broad range of security issues and environments in their daily work, giving them experience that would be difficult to accumulate working within a single company. In addition, they are up-to-date on—and conversant in—the myriad compliance and auditing requirements of industries and the federal government. Because security is its core business, Global Security Consulting can justify continued investment in highly qualified staff, ongoing training, and state-of-the-art assessment and monitoring technology. In addition, technology, methodology, and personnel are already proven and in place, saving valuable time when deploying a layered defense solution.

VeriSign's iDefense research team provides comprehensive, actionable intelligence on network-based security threats and vulnerabilities for financial services firms, government agencies, retailers, and other large organizations. VeriSign® iDefense® researchers work in tandem with staff from VeriSign Security Operations Centers to provide sophisticated insight into emerging threats.

For more information about VeriSign's Layered Security solutions, please contact a VeriSign representative at 650-426-5310.

+ About VeriSign

VeriSign operates digital infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

00024561 5-9-2007